The source code of the e-voting system is problematic, and that's not just about security (interview with Christian Killer, Burkhard Stiller)

Killer, Christian ; Stiller, Burkhard

The source code of the e-voting system is problematic, and that's not just about security (interview with Christian Killer, Burkhard Stiller)

Killer, Christian ; Stiller, Burkhard

Neue Zürcher Zeitung

Der Quellcode des E-Voting-Systems ist problematisch, und das hat nicht nur mit Sicherheit zu tun

E-Voting ist umstritten – unter anderem, weil Sicherheitslücken wohl nie ganz ausgeschlossen werden können. Aber Experten sehen im Quellcode des Schweizer Systems noch ganz andere Probleme.

Marie-José Kolly (Text) / Christian Kleeb (Teaserbild) 25.2.2019, 18:16 Uhr

Die Schweizer Post hat zusammen mit der spanischen Firma Scytl ein E-Voting-System für die Schweiz entwickelt und den Quellcode für registrierte Nutzer offengelegt. So können Hacker das System im Rahmen eines sogenannten Intrusionstests prüfen, denn Kritiker warnen schon lange vor Sicherheitslücken.

Nun gelangte der Quellcode schon vor Beginn des Tests an die Öffentlichkeit. Kryptografen, Informatiker und Experten auf der ganzen Welt üben Kritik daran.

Aber wo genau liegen die Probleme beim Quellcode von Schweizer Post und Scytl? Wir haben zwei Informatiker der Universität Zürich gefragt: Burkhard Stiller, Professor, und Christian Killer, Doktorand.

1. Der Code ist nicht übersichtlich aufgebaut

«Es ist schwierig, diesen Quellcode zum Laufen zu bringen», sagt Christian Killer. Gut 420 000 Zeilen Code verteilen sich auf Hunderte von Dateien und Module. Module sind Code-Pakete, die eine bestimmte Aufgabe erfüllen. Und damit die Software auf einem Computer zum Laufen kommt, müssen diese Module richtig zusammenspielen – das System ist also hochkomplex.

Wenn Experten wie beim vorliegenden Intrusionstest ein System prüfen sollen, muss es systematisch aufgebaut sein. Aber die Art und Weise, wie der vorliegende Code aufgebaut ist, verhindert das.

Das komplexe System ist zudem sehr umfangreich: Burkhard Stiller erklärt, dass komplexere Masterarbeiten seiner Studierenden etwa 10 000 Zeilen Code umfassen. Solche Arbeiten zu testen und auf eventuelle Fehler zu prüfen, nehme sehr viel Zeit in Anspruch, und manchmal tauchten Fehler auch erst nach einiger Zeit auf.

Eine Fehlerfrei-Garantie: Das gebe es nur in Ausnahmefällen. Auditing-Firmen könnten unter Umständen bei Code-Paketen bis zu 100 Zeilen Fehlerfreiheit garantieren, sagt Stiller. Und das schafften nur mehrere versierte Experten gemeinsam. Denn das Überprüfen von IT-Systemen brauche Kenntnisse in Kryptografie; darin, wie man effizienten Code schreibt; darin, wie man «Nebenwirkungen» des Codes entdeckt, die nicht intendiert sind; darin, wie man Code in einem Betriebsumfeld aufsetzt; darin, wie Anwender auf die Software reagieren …

Den E-Voting-Quellcode à 420 000 Zeilen zu prüfen, ist also ein gewaltiges Unterfangen.

2. Die Dokumentation entspricht nicht den Standards

Die Verordnung der Bundeskanzlei über die elektronische Stimmabgabe gibt vor, dass der Quellcode eines E-Voting-Systems offengelegt werden muss. Aber nicht nur: Der Code muss auch «nach besten Praktiken aufbereitet und dokumentiert werden», und seine Dokumentation «muss die Relevanz der einzelnen Teile des Quellcodes für die Sicherheit der elektronischen Stimmabgabe erklären».

Das ist hier aber nur zum Teil gegeben:

«Die Dokumentation wirkt nicht komplett», sagt Christian Killer. Es sehe für ihn so aus, als wäre sie schnell für Experten zusammengestellt worden, um möglicherweise die Vorgabe der Bundeskanzlei zu erfüllen.

Denn es sei auch für ihn als Experten schwierig, aus der Dokumentation herauszulesen, wie die einzelnen Komponenten des Codes funktionierten und zusammenspielten. Burkhard Stiller ergänzt: «Die Zielgruppe der Dokumentation sind hochspezialisierte Experten.»

Ein Grund dafür könnte sein, dass eine private Firma wie Scytl kein Interesse daran hat, die Grundlage ihres Geschäftsmodells offenzulegen und zu dokumentieren. «So werden Abhängigkeiten geschaffen», sagt Christian Killer. Und die Vorgehensweise widerspricht zumindest implizit der Transparenzvorschrift der Bundeskanzlei.

3. Die Bausteine müssen einzeln konfiguriert werden

Da sind also Hunderttausende Codezeilen in Hunderten von Modulen und eine unvollständige Dokumentation. Nun müssen jedoch die Module vom Nutzer auf verschiedene Art und Weise konfiguriert, also parametrisiert werden. Man muss also bestimmen, ob es sich um eine Abstimmung oder um eine Wahl handelt. Ob sie auf Gemeinde- oder auf Bundesebene stattfindet. Ob gewisse Code-Teile in einem bestimmten Fall verwendet werden oder nicht.

Code müsste eigentlich so geschrieben sein, dass er kaum falsch konfiguriert werden kann, sagen die Experten der Universität Zürich. Das System der Post in der vorliegenden Fassung aber überlässt es dem Nutzer (jetzt: Hacker, in Zukunft: die Kantone), das System richtig zu konfigurieren.

Und zwar muss jeder Teil des Codes richtig konfiguriert werden, sonst wird das System vulnerabel für Angreifer:

Falsch konfigurierter Code macht es externen Angreifern unter Umständen möglich, abgegebene Stimmen zu ändern. Und interne Angreifer könnten Teile des Systems absichtlich falsch konfigurieren – weil die Konfiguration so komplex ist, wäre es sogar plausibel, anzunehmen, die falsche Konfiguration sei unabsichtlich erfolgt. Stiller sagt dazu: «Die Analogie ist leicht übertrieben, aber es ist, als bekäme man einen Sack voller Lego-Bausteine und dazu keinen Bauplan.»

Das System sei so undurchsichtig, dass man mögliche Fehler oder Lücken darin gar nicht auf den ersten Blick sehen könne, erklären die beiden Experten. Es sei denn, man beschäftige sich tagelang mit diesen Modulen und Codezeilen.

4. Die Dokumentation darf nicht zitiert werden

Der Quellcode kann von jeder Person eingesehen werden. Aber die Dokumentation dazu enthält einen Disclaimer: Man darf sie – oder Elemente daraus – nicht verwenden, nicht nachbauen, weiter verwenden oder referenzieren.

«Das ist sehr merkwürdig», sagt Killer. Man dürfe sich also offiziell nicht über den Quellcode und seine Dokumentation austauschen. Als Hacker oder IT-Experte dürfe man seine Erkenntnisse über den Code nur an die Urheber weitergeben.

Die beiden Experten können sich ein Lächeln nicht verkneifen, als sie darüber sprechen. Die Vorgabe scheint absurd: Sie macht den Austausch zwischen Experten theoretisch unmöglich. Es ist nicht erlaubt, was in der Welt derer, die Code schreiben und prüfen, selbstverständlich ist: gemeinsam nach Fehlern zu suchen, auf der Arbeit anderer aufzubauen.

Der Disclaimer widerspricht auch einer weiteren Vorgabe der Bundeskanzlei: «Jeder und jede darf den Quellcode zu ideellen Zwecken untersuchen, verändern, kompilieren und ausführen sowie dazu Studien verfassen und diese publizieren. Der Eigner des Quellcodes kann dessen Nutzung zu anderen Zwecken erlauben.»

E-Voting spaltet die Fachwelt
Hernani Marques ist Experte für Computersicherheit. Er sagt: «Es wird nie ein elektronisches Abstimmungssystem geben, das absolut sicher ist». Aber die Meinungen unter IT-Fachleuten sind geteilt.
Lukas Leuzinger / 11.5.2018, 05:30

Das grosse Zögern bei der Energiewende
Bisher sind erst 1,8 Millionen Einwohner von strengen Energie-Vorschriften betroffen. Wie in Bern könnte es auch in anderen Kantonen zu Widerstand gegen strenge Auflagen kommen.
Daniel Gerny / 12.2.2019, 17:24